12.

CLAIMS

13. An access control protocol between an electronic key and an electronic lock performing access control, in which protocol, following presentation of said electronic key to said electronic lock, a random variable message prompting authentication of the electronic key is transmitted from said electronic lock to said electronic key, wherein, on receiving said random variable message prompting authentication, said protocol consists of at least, in succession:

- calculating and transmitting from said electronic key to said electronic lock a digital signature value of said random variable message prompting authentication based on a private signature key and specific authentication data, said specific authentication data transmitted by said electronic key to said electronic lock consisting of at least one public key certificate associated with said private signature key, said public key certificate consisting of a digital signature value of at least one validity time period relating to a right of access and of said public key, said signature value being calculated from another private signature key associated with another public key, and, after reception by said electronic lock of said signature value and said specific authentication data:

- verification by said electronic lock of the authenticity of said signature value as a function of said specific authentication data and, in response to a positive or negative result of said verification:

- acceptance or respectively refusal of said access.

14. The protocol according to claim 13, wherein said step of verification of said signature value by said electronic lock includes, in succession:

- verification by said electronic lock of the authenticity of said specific authentication data based on

comparison with reference data and, in the event of a positive result of said comparison:

- verification by said electronic lock of said signature value as a function of said specific authentication data.

15. The protocol according to claims 13 and 14, wherein said step of verification by said electronic lock of the authenticity of said specific authentication data consists of checking said validity time period associated with said public key.

16. The protocol according to claim 14, wherein validity time period includes a plurality of non-contiguous time intervals.

17. The protocol according to claim 14. wherein each validity time period consists of at least one time interval having two limits each expressed as a date in terms of day, month, year and a time in terms of hour, minute, second.

18. The protocol according to claim 13, wherein said random variable message prompting authentication is a function of an identification value of said electronic lock and a continuously increasing variable value.

19. The protocol according to claim 13, wherein, after reception of said random variable message prompting authentication by said electronic key but before the step of calculation and transmission of a signature value by said electronic key, said electronic key having an internal clock, said protocol further consists of an auxiliary verification step for authorising calculation of the signature of said random variable message prompting authentication, said auxiliary verification step consisting of:

- using the other public key associated with said other private signature key to verify said public key certificate and said validity time period associated with

said public key against said internal clock, to verify the validity of said public key,

- verifying the association of said private signature key and said public key, whose validity has been verified in the preceding step, and, on the basis of positive and negative result criteria, for the preceding two verification steps:

- continuing or respectively interrupting said access control protocol.

20. The protocol according to claim 13 further comprising a plurality of tests limiting all attack outside said validity time period, which tests are performed during said step of verification by said electronic lock of the authenticity of said signature value, after said step of verification by said electronic lock of the authenticity of the specific authentication data consisting of checking said validity time period associated with said public key but before said step of verification by said electronic lock of the authenticity of said signature value, said protocol further comprising a plurality of tests limiting any attack outside said validity time period.

21. The protocol according to claim 12 further comprising, before said step of calculation and transmission from said electronic key to said electronic lock of a signature value of said random variable message prompting authentication and specific authentication data, said electronic key including a real-time clock:

- a step of testing if a time variable delivered by said real-time clock is inside said validity time period and, in the event of a negative result of said test:

- a step of invalidation of said electronic key interrupting said access control and leading to refusal of said access by said electronic lock.

22. An electronic key comprising cryptographic

calculation means and message or data transmission means for implementing an access control protocol between an electronic key and an electronic lock performing access control, in which protocol, following presentation of said electronic key to said electronic lock, a random variable message prompting authentication of the electronic key is transmitted from said electronic lock to said electronic key and on receiving said random variable message prompting authentication, said protocol consists of at least, in succession, calculating and transmitting from said electronic key to said electronic lock a digital signature value of said random variable message prompting authentication based on a private signature key and specific authentication data, said specific authentication data transmitted by said electronic key to said electronic lock consisting of at least one public key certificate associated with said private signature key, said public key certificate consisting of a digital signature value of at least one validity time period relating to a right of access and of said public key, said signature value being calculated from another private signature key associated with another public key, and, after reception by said electronic lock of said signature value and said specific authentication data, verification by said electronic lock of the authenticity of said signature value as a function of said specific authentication data and, in response to a positive or negative result of said verification, acceptance or respectively refusal of said access, for controlling access to an electronic lock by said electronic key, wherein, in addition to a central processor unit (CPU), said cryptographic calculation means include at least:

- a protected access memory area for storing at least one private signature key and specific authentication data, said specific authentication data

consisting of at least one public key certificate consisting of a digital signature value of at least one validity time period relating to a right of access and said public key, and

- a read-only memory used to call programs for calculating the digital signature value of a random variable message delivered by said electronic lock using said private signature key.

A1 cont

23. 22. An electronic lock comprising cryptographic calculation means and message or data transmission means for implementing an access control protocol between an electronic key and an electronic lock performing access control, in which protocol, following presentation of said electronic key to said electronic lock, a random variable message prompting authentication of the electronic key is transmitted from said electronic lock to said electronic key and on receiving said random variable message prompting authentication, said protocol consists of at least, in succession, calculating and transmitting from said electronic key to said electronic lock a digital signature value of said random variable message prompting authentication based on a private signature key and specific authentication data, said specific authentication data transmitted by said electronic key to said electronic lock consisting of at least one public key certificate associated with said private signature key, said public key certificate consisting of a digital signature value of at least one validity time period relating to a right of access and of said public key, said signature value being calculated from another private signature key associated with another public key, and, after reception by said electronic lock of said signature value and said specific authentication data, verification by said electronic lock of the authenticity of said signature value as a function of said specific authentication data and, in response to a

positive or negative result of said verification, acceptance or respectively refusal of said access, for controlling access to said electronic lock by an electronic key, wherein, in addition to a central processor unit, said calculation means include at least:

- a protected access memory area for storing at least one public signature verification key, and
- a read-only memory used to call signature verification programs based on said at least one public key.